Università degli Studi di Milano

Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2005–2006 docente: Stefano Ferrari

25.03.2006 — Soluzione della prima parte — versione A

valutazioni **1** (5) ______ **2** (5) ______ **3** (5) ______ **4** (4) ______ **5** (4) ______ **6** (9) ______

Cognome ____________________ **Nome** ____________________

Matricola ____________________ **Firma** ____________________

Esercizio 1

Per ogni numero k, calcolare il corrispondente numerale nella base n indicata:

a) $k = (431)_5$, $n = 10$

b) $k = (25)_{10}$, $n = 2$

c) $k = (3\mathrm{F})_{16}$, $n = 2$

d) $k = (107)_8$, $n = 2$

e) $k = (124)_5$, $n = 2$

f) $k = (11101011)_2$, $n = 16$

Soluzione

a) $(431)_5 = 4 \cdot 5^2 + 3 \cdot 5^1 + 1 \cdot 5^0 = 4 \cdot 25 + 3 \cdot 5 + 1 \cdot 1 = 100 + 15 + 1 = 116$

$(431)_5 = (116)_{10}$

b)

quoziente	resto
25	
12	1
6	0
3	0
1	1
0	1

$(25)_{10} = (11001)_2$

c)

base 16	3	F
base 2	0011	1111

$(3\mathrm{F})_{16} = (111111)_2$

d)

base 8	1	0	7
base 2	001	000	111

$(107)_8 = (1000111)_2$

e) $(124)_5 = 1 \cdot 5^2 + 2 \cdot 5^1 + 4 \cdot 5^0 = 1 \cdot 25 + 2 \cdot 5 + 4 \cdot 1 = 25 + 10 + 4 = 39$

quoziente	resto
39	
19	1
9	1
4	1
2	0
1	0
0	1

$(124)_5 = (100111)_2$

f)

base 2	1110	1011
base 16	E	B

$(11101011)_2 = (\mathrm{EB})_{16}$

Esercizio 2

Dati $a = 21$, $b = -7$ e $n = 5$, calcolare in complemento a 2 a n bit, specificando se si verifica un overflow:

1. le stringhe binarie s_a e s_b che codificano rispettivamente a e b;
2. la somma delle stringhe binarie s_a e s_b;
3. la differenza delle stringhe binarie s_a e s_b.

Soluzione

Con la codifica in complemento a 2 a 5 bit possono essere rappresentati tutti i numeri interi compresi fra -2^{5-1} e $2^{5-1} - 1$. Possono pertanto essere rappresentati senza causare overflow tutti e soli i numeri x che rispettano la condizione $-16 \leq x \leq 15$.

1. $2^n + a = 2^5 + 21 = 53$. Codificando 53 in binario e troncando tale codifica a 5 bit si ottiene: $s_a = 10101$.

Poiché $a = 21 > 15$, si è verificato un overflow.

$2^n + b = 2^5 - 7 = 25$. Codificando 25 in binario e troncando tale codifica a 5 bit si ottiene: $s_b = 11001$.

Poiché $-16 \leq -7 \leq 15$, non si è verificato un overflow.

2. La somma binaria di 10101 e 11001, troncata a 5 bit è: $s_a + s_b = 01110$.

   Poiché s_a e s_b hanno il primo bit uguale, ma diverso dal primo bit della loro somma, 01110, si è verificato un overflow.

3. La differenza viene calcolata come somma di s_a e di $-s_b$.

$$
\begin{array}{rcl}
11001 & & \text{sottraendo, } s_b \\
00110 & + & \text{negazione delle cifre di } s_b,\ \overline{s_b} \\
1 & = & \\
\hline
00111 & + & -s_b \\
10101 & = & s_a \\
\hline
11100 & & s_a - s_b
\end{array}
$$

   Poiché s_a e s_b hanno il primo bit uguale, non si è verificato un overflow.

Esercizio 3

Una azienda produce palloncini con le seguenti caratteristiche:

- colore: bianco, rosso, giallo, verde;
- forma: sferica, allungata, ondulata;
- dimensione: piccolo, grande.

I palloncini vengono venduti confezionati in un sacchetto che ne contiene 7, tutti della stessa dimensione, ma con almeno una delle altre caratteristiche diversa.

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (colore, forma, dimensione);

b) il numero di bit necessari per codificare un palloncino;

c) il numero di bit necessari per codificare le possibili confezioni.

Soluzione

a)
- 4 colori: $\lceil \log_2 4 \rceil = 2$ bit;
- 3 forme: $\lceil \log_2 3 \rceil = 2$ bit;
- 2 dimensioni: $\lceil \log_2 2 \rceil = 1$ bit.

b) Ci sono $4 \times 3 \times 2 = 24$ varianti di palloncino, quindi servono $\lceil \log_2 24 \rceil = 5$ bit.

c) Le confezioni sono sono composte da 7 palloncini della stessa dimensione. Le ripetizioni non sono ammesse in quanto tutte le altre caratteristiche (superficie e colore) devono essere diverse. Non vi sono specifiche esplicite riguardo all'importanza dell'ordine dei palloncni nella stessa confezione, e il confezionamento in sacchetti fa pensare che l'ordine non sia da tenere in considerazione. Quindi, per ogni dimensione, si potranno avere un numero di confezioni pari al numero di combinazioni semplici di 12 oggetti (4 colori $\times$ 3 forme) su 7 posti.

$$
\begin{aligned}
C(12, 7) &= \frac{12!}{(12-7)! \cdot 7!} = \\
&= \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2} = \\
&= 11 \cdot 9 \cdot 8 = 2^3 \cdot 99
\end{aligned}
$$

Poiché si hanno 2 differenti dimensioni, in totale si avranno quindi $2 \cdot 2^3 \cdot 99 = 2^4 \cdot 99$ possibili confezioni. Poiché la prima potenza di 2 che supera 99 è 2^7, per codificare le possibili confezioni serviranno $\lceil \log_2(2^4 \cdot 99) \rceil = \lceil \log_2 2^4 + \log_2 99 \rceil = \lceil 4 + \log_2 99 \rceil = 4 + \lceil \log_2 99 \rceil = 4 + 7 = 11$ bit.

Esercizio 4

Dimostrare, tramite tavola di verità, ***se*** la seguente formula è una tautologia:

a) $(\neg p \lor q) \rightarrow ((\neg q \land r) \leftrightarrow \neg r)$

Soluzione

La tabella di verità è riportata in figura 1. Poiché almeno una interpretazione rende vera la proposizione data, essa non è una tautologia.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non lavora, ozi, e viceversa):

a) se Carlo lavora, Bice e Antonio oziano;

b) Bice ozia se e solo se Carlo lavora;

c) Carlo non lavora, Bice e Antonio sì;

d) Antonio o Bice oziano;

e) Carlo lavora solo se anche Bice fa lo stesso;

p	q	r	$\neg p$	$\neg p \vee q$	$\neg q$	$\neg q \wedge r$	$\neg r$	$\beta \leftrightarrow \neg r$	$\alpha \to \gamma$
F	F	F	V	V	V	F	V	F	F
F	F	V	V	V	V	V	F	F	F
F	V	F	V	V	F	F	V	F	F
F	V	V	V	V	F	F	F	V	V
V	F	F	F	F	V	F	V	F	V
V	F	V	F	F	V	V	F	F	V
V	V	F	F	V	F	F	V	F	F
V	V	V	F	V	F	F	F	V	V
				α		β		γ	

Figura 1: Tabella di verità della proposizione dell'esercizio 4.

Soluzione

Dati i seguenti simboli proposizionali:

a	Antonio lavora
$\neg a$	Antonio ozia
b	Bice lavora
$\neg b$	Bice ozia
c	Carlo lavora
$\neg c$	Carlo ozia

le frasi dell'esercizio possono essere formalizzate tramite le seguenti proposizioni:

a) $c \to (\neg b \wedge \neg a)$

b) $\neg b \leftrightarrow c$

c) $\neg c \wedge b \wedge a$

d) $\neg a \vee \neg b$

e) $c \to b$

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

a) **Ip1** $a \vee b$
Ip2 $a \to (\neg a \wedge c)$
Tesi $\neg b \to b$

b) **Ip1** a
Ip2 $a \to (b \wedge c)$
Tesi $\neg c \to \neg b$

c) **Ip1** $a \vee b$
Ip2 $b \vee (\neg a \wedge (\neg a \vee c))$
Tesi b

Soluzione

a)

(1)	$a \to (\neg a \wedge c)$	Ip2
(2)	$(a \to \neg a) \wedge (a \to c)$	Distrib. conseguenze (1)
(3)	$a \to \neg a$	Elim. congiunzione (2)
(4)	$\neg a \vee \neg a$	Def. implicazione (3)
(5)	$\neg a$	Idempotenza (4)
(6)	$a \vee b$	Ip1
(7)	$\neg a \to b$	Def. implicazione (6)
(8)	b	Modus Ponens (5) e (7)
(9)	$b \to (\neg b \to b)$	Ex falso sequitur quodlibet
(10)	$\neg b \to b$	Modus Ponens (8) e (9)

b)

(1)	a	Ip1
(2)	$a \to (b \wedge c)$	Ip2
(3)	$b \wedge c$	Modus Ponens (1) e (2)
(4)	c	Elim. congiunzione (3)
(5)	$c \to (c \vee \neg b)$	Introd. disgiunzione
(6)	$c \vee \neg b$	Modus Ponens (4) e (5)
(7)	$\neg c \to \neg b$	Def. implicazione (6)

È anche valida la dimostrazione alternativa riportata in figura 2.

c) Una possible soluzione è riportata in figura 3.

(1)	a	Ip1
(2)	$b \rightarrow a$	Verum sequitur a quodlibet (1)
(3)	$a \rightarrow (b \wedge c)$	Ip2
(4)	$(a \rightarrow b) \wedge (a \rightarrow c)$	Distrib. delle conseguenze (3)
(5)	$a \rightarrow c$	Elim. congiunzione (4)
(6)	$b \rightarrow c$	Sillogismo ipotetico (2) e (5)
(7)	$\neg c \rightarrow \neg b$	Contrapposizione (6)

Figura 2: Una possibile soluzione alternativa dell'esercizio 6b.

(1)	$b \vee (\neg a \wedge (\neg a \vee c))$	Ip2
(2)	$(b \vee \neg a) \wedge (b \vee (\neg a \vee c))$	Distributività (1)
(3)	$b \vee \neg a$	Elim. congiunzione (2)
(4)	$\neg b \rightarrow \neg a$	Def. implicazione (3)
(5)	$a \rightarrow b$	Contrapposizione (4)
(6)	$a \vee b$	Ip1
(7)	$\neg a \rightarrow b$	Def. implicazione (6)
(8)	b	Dim. per casi (5) e (7)

Figura 3: Una possibile soluzione dell'esercizio 6c.